14463

aetna℠

[DATE]

[MEMBER NAME]
[ADDRESS 1]
[CITY] [STATE], [ZIP]

RE: Notice of BenefitMall Data Breach

Dear [redacted]:

We were recently notified of a privacy breach involving your personal information and are writing to provide information to you about it. The privacy breach occurred at Centerstone Insurance and Financial Services, Inc. d/b/a BenefitMall, who serves as a general agent as well as a third-party vendor that Aetna utilizes to provide administrative services related your employee benefits (e.g., enrollment and billing services).

Here is what happened:
On December 11, 2018, BenefitMall notified us that phishing attacks, which occurred between approximately June 2018 and October 19, 2018, compromised certain BenefitMall employee email accounts containing Aetna member information. BenefitMall also informed us that it became aware of these attacks on October 11, 2018 and that the incident has since been contained. Based upon its investigation, BenefitMall determined that an unauthorized third party was able to obtain correspondence containing personal information.

This incident did not involve any Aetna system or application.

How Aetna responded:
On December 18, 2018, BenefitMall provided us with a cursory list of affected individuals. Because the list lacked certain important information, we promptly initiated a review of this list to identify Aetna members, their benefit plans, and their addresses. We have also had several communications with BenefitMall regarding this breach to assist in our own investigation and review of the matter.

Types of information involved:
BenefitMall notified us that the affected correspondence generally included names, addresses, Social Security numbers, dates of birth, zip codes, bank account numbers, plan descriptions, premium payment amounts, and health plan beneficiary numbers.

Protection of your information:
In light of the phishing attacks that occurred at BenefitMall, we are offering, at no cost, two (2) years of Equifax Credit Watch™ Gold with 3-in-1 Monitoring Identity Theft Protection. To take advantage of this protection, please follow the enclosed instructions and activate your coverage no later than [_____], 2019. Your activation code is: [_____]. We have also enclosed some general information about steps you can take to guard against identity theft and fraud.

Aetna takes its obligation to protect the privacy and confidentiality of its members' personal information very seriously and expects its vendors to do the same. Accordingly, we have reviewed BenefitMall's efforts to remediate the breach and ensure that it does not happen again.

We sincerely regret that this incident occurred. If you have any questions, please call [_____] during the hours of [_____] EST.

Sincerely,

Tracey E. Scraba
Chief Privacy Officer

Please find below Aetna's responses to the below questions on the Massachusetts Office of Consumer Affairs and Business Regulation's Online Data Breach Notification Form.

Please give a detailed explanation of how the data breach occurred.*

On December 11, 2018, Centerstone Insurance and Financial Services, Inc. d/b/a BenefitMall ("BenefitMall"), a general agent who also acts as a third-party vendor that Aetna utilizes to provide administrative services related to employee benefits (e.g., enrollment and billing services), notified Aetna that phishing attacks, which occurred between approximately June 2018 and October 19, 2018, had compromised certain BenefitMall employee email accounts containing Aetna member information. BenefitMall has a primary place of business at 12404 Park Central Drive, Suite 400S Dallas, Texas 75251, and Aetna considers Tiffany Stiller with a phone number of (818) 226-6517 Ext 286517 to be its primary contact at BenefitMall.

BenefitMall also informed Aetna that it became aware of these attacks on October 11, 2018 and that the incident has since been contained. Based upon its investigation, BenefitMall determined that an unidentified, unauthorized third party was able to obtain correspondence containing personal information. BenefitMall informed Aetna that the affected correspondence generally included names, addresses, Social Security numbers, dates of birth, zip codes, bank account numbers, plan descriptions, premium payment amounts, and health plan beneficiary numbers.

BenefitMall informed Aetna that it retained a cybersecurity forensics firm to assist in a thorough investigation of the incident and that it has implemented additional security measures designed to protect employee email accounts, including two-factor authentication for access to its email system. Based upon conversations with BenefitMall, Aetna's understanding is that the information was not encrypted and that the information has not been recovered. Additionally, BenefitMall informed Aetna that it reported the incident to law enforcement.

Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring.*

On December 18, 2018, BenefitMall provided Aetna with a cursory list of affected individuals. Because the list lacked certain important information, Aetna promptly initiated a review of this list to identify Aetna members, their benefit plans, and their addresses. The list Aetna received from BenefitMall did not include this information and contained a large number of duplicates. Aetna worked diligently, and expended considerable time and resources, to review the limited, inconsistent personal information included in the BenefitMall list to locate the addresses of the individuals listed, so that Aetna could provide notice to affected individuals as soon as possible. Aetna recently determined that this breach impacted approximately nine (9) Massachusetts residents who are fully-insured members of Aetna health benefit plans. Aetna has also had several communications with BenefitMall regarding this breach to assist in its own investigation and review of the matter. Additionally, Aetna has reviewed BenefitMall's efforts to remediate the breach and ensure that it does not happen again.

In accordance with its obligations set forth at 45 C.F.R. § 164.404 (notifications to individuals by a HIPAA covered entity) and Massachusetts law, Aetna is issuing notification to the impacted members of the fully-insured plans by first class U.S. mail. Aetna commenced the mailing of all such notifications on January 30, 2019. In addition, Aetna will be offering each such individual, at no cost, two (2) years of Equifax Credit Watch™ Gold with 3-in-1 Monitoring Identity Theft Protection. Aetna is also notifying other federal and state regulatory agencies as required by law.

Reference Guide

Monitor Account Statements. Remember to look at your account statements regularly to be sure they are correct.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open and medical bills you do not recognize. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

If you find items you don't understand on your report, call the relevant credit bureau at the number given on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission. If you detect any unauthorized transactions in your financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the FTC. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft (including information about fraud alerts and security freezes):

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For a summary of your rights under the federal Fair Credit Reporting Act, please visit: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Place a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus. [*The table below contains the contact information relevant to fraud alerts.*]

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	877-478-7625	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Place a "Security Freeze" on Your Credit File (for Non-Massachusetts Residents). You also may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. There is no longer a fee for placing, lifting, and/or removing a security freeze. Unlike a fraud alert, you must place a security freeze on your credit file at each credit bureau individually. Since the instructions for establishing a security freeze differ from state to state, please contact the three national credit bureaus to find out more information. [*The table below contains the contact information relevant to security freezes.*]

Equifax	P.O. Box 105788 Atlanta, Georgia 30348	877-478-7625	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Attn: Security Freeze P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

The credit bureaus may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth

- Your complete address including proof of current address, such as current utility bill or telephone bill
- If you have moved in the past two (2) years, give your previous addresses where you have lived for the past two years
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

Additional Information for Maryland Residents.

You can also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office:

Office of the Maryland Attorney General
Identity Theft Unit
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
1-888-743-0023
idtheft@oag.state.md.us
http://www.marylandattorneygeneral.gov

Additional Information for North Carolina Residents.

You can also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov

Additional Information for Rhode Island Residents.

Under Rhode Island law, you have the right to file a police report regarding this incident and obtain a copy of it.

You can contact the Rhode Island Attorney General to learn more about how to protect yourself from becoming a victim of identity theft:

Office of the Rhode Island Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401) 274-4400
consumers@riag.ri.gov
http://www.riag.ri.gov

Additional Information for Massachusetts Residents.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. There is no longer a fee for placing, lifting, and/or removing a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348

Experian Security Freeze P.O. Box 9554 Allen, TX 75013

Trans Union Security Freeze Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19022-2000

In order to request a security freeze, you will need to provide the following information:
1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.